



IT Security Handbook

Personnel Security

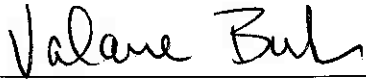
ITS-HBK- 2810.13-01
Effective Date: 20110506
Expiration Date: 20130506
Responsible Office: OCIO/ Deputy CIO for Information Technology Security

ITS Handbook (ITS-HBK-2810.13-01)
Personnel Security

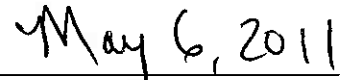
Distribution:

NODIS

Approved



Valarie Burks
Deputy Chief Information Officer for
Information Technology Security



Date

Change History

Version	Date	Change Description
1.0	5/2/11	Initial Draft

Table of Contents

Change History	3 -
1 Introduction and Background	5 -
2 Position Categorization (PS-2)	5 -
3 Personnel Screening (PS-3)	6 -
4 Personnel Termination (PS-4)	6 -
5 Personnel Transfer (PS-5)	6 -
6 Access Agreements (PS-6)	6 -
7 Third-Party Personnel Security (PS-7)	6 -
8 Personnel Sanctions (PS-8)	7 -
9 Organizationally Defined Values	8 -

1 Introduction and Background

- 1.1 - NASA requirements for protecting the security of NASA information and information systems are derived from National Institute of Standards and Technology (NIST) guidance. Information System Owners (ISOs) and other personnel responsible for the protection of NASA information or information systems shall follow NIST guidance in the proper security categorization (*Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization for Federal Information and Information Systems*), and in the selection and implementation of information security controls (*FIPS 200, Minimum Security Requirements for Federal Information and Information Systems* and *NIST Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems and Organizations*), in a manner consistent with the Risk Management Framework (*NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems*).
- 1.2 - This handbook augments NIST guidance by providing NASA-specific requirements, procedures and recommendations, where applicable. NASA-specific guidance does not negate NIST guidance, unless explicitly stated.
- 1.3 - *NASA Policy Directive (NPD) 2810.1, NASA Information Security Policy, NASA Procedural Requirements (NPR) 2810.1, Security of Information Technology*, and the collection of 2810 Information Technology Handbooks (ITS-HBK) satisfy the policy and procedure controls of *NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations*.
- 1.4 - *NPR 2810.1, Security of Information Technology*, designates this handbook as a guide of NASA's Personnel Security (PS) information security controls.
- 1.5 - The terms "shall" and "may" within this handbook are used as defined in *ITS-HBK-0001, Format and Procedures for IT Security Policies and Handbooks*.
- 1.6 - The Personnel Security control family relates to the security activities that surround various facets of the employment life cycle (i.e., initial employee screening, position categorization, authority delegation, sanctioning, transfers, and termination). Personnel Security applies to both direct employees of the Agency as well as contracted personnel, and service bureaus.
- 1.7 - **Applicable Documents**
- *NASA Federal Acquisitions Regulation (FAR) Supplement*
 - *NPD 2810.1, NASA Information Security Policy*
 - *NPR 1441.1, NASA Records Retention Schedules*
 - *NPR 1600.1, NASA Security Program Procedural Requirements*
 - *NPR 2810.1, Security of Information Technology*
 - *ITS-HBK-0001, Format and Procedures for IT Security Policies and Handbooks*
 - *FIPS 199, Standards for Security Categorization for Federal Information and Information Systems*
 - *FIPS 200, Minimum Security Requirements for Federal Information and Information Systems*
 - *NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems*
 - *NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations*

2 Position Categorization (PS-2)

- 2.1 - **Roles and Responsibilities**
- 2.1.1 *The Information System Owner (ISO) shall:*
- 2.1.1.1 - Ensure positions related to their information systems are assigned a risk designation of High, Medium, or Low for all positions in accordance with *NPR 1600.1*.
 - 2.1.1.2 - Ensure the periodic review and revision of risk designation for positions under their supervision, in manner - consistent with organizationally defined values. -

3 Personnel Screening (PS-3)

3.1 Roles and Responsibilities

3.1.1 The ISO shall: -

- 3.1.1.1 - Ensure that personnel screening and any re-screening is consistent with *NPR 1600.1*, and organizationally defined values. -
- 3.1.1.1.1 - Screening criteria includes establishing the suitability/eligibility for the positions and the minimum requiring investigation based on the position categorization. -

4 Personnel Termination (PS-4)

4.1 Roles and Responsibilities

4.1.1 The ISO shall: -

- 4.1.1.1 - Ensure, upon termination of individual employment, termination of information system access. -
- 4.1.1.2 - Ensure completion of the "Employee Termination" request in the Identity Management and Account Exchange (IdMAX) system. -
- 4.1.1.3 - Retrieve all security related NASA information and information system-related property and materials. -
- 4.1.1.4 - Retain and ensure access to all NASA information and information system formally controlled by the terminated individual. -

5 Personnel Transfer (PS-5)

5.1 Roles and Responsibilities

5.1.1 The ISO shall: -

- 5.1.1.1 - Review and update information system logical and physical access authorizations for transferred individuals. -
- 5.1.1.2 - Manage opening new accounts and closing old accounts. -
- 5.1.1.3 - Manage changing system authorizations. -
- 5.1.1.4 - Manage the return of and issuing of new keys, building passes, etc. -
- 5.1.1.5 - Provide access to official records that the employee had access to at previous work locations or on prior accounts, in accordance with *NPR 1441.1*. -

6 Access Agreements (PS-6)

6.1 Roles and Responsibilities

6.1.1 The ISO shall: -

- 6.1.1.1 - Ensure signed access agreements are established, updated, and reviewed in a manner consistent with organizationally defined values. -

7 Third-Party Personnel Security (PS-7)

7.1 Roles and Responsibilities

7.1.1 The Center Chief Information Security Officer (CISO) shall: -

- 7.1.1.1 - Provide oversight of the security implementation of third-party contracts including external/contractor systems at their Center. -

7.1.2 The Organization Computer Security Official (OCSO) shall: -

- 7.1.2.1 - Provide oversight of the security implementation of third-party contracts including external/contractor systems at their organization. -

7.1.3 The ISO shall: -

- 7.1.3.1 - Ensure NASA personnel security requirements are met by third party personnel with contracts including the provision of *NASA FAR supplement 1852-204-76*, and *NPR 1600.1*. -

- 7.1.3.1.1 *NASA Far supplement 1852-204-76* is included in all contracts related to systems and services that provide or use NASA information and information services.

8 Personnel Sanctions (PS-8)

8.1 Roles and Responsibilities

8.1.1 *The Center CISO shall:*

- 8.1.1.1 Report security violations at their Center to the appropriate organizations and officials that may need to take security corrective actions.
 - 8.1.1.1.1 If appropriate for disciplinary or adverse actions, recommendations and actions should be provided in accordance with the NASA Human Capital policies and requirements.
 - 8.1.1.1.2 If potential for criminal action, information to the OIG for investigative and follow-up actions should be provided in accordance with the OIG policies, requirements and procedures.

8.1.2 *The OCSO shall:*

- 8.1.2.1 Report security violations in their organization to the appropriate organizations and officials that may need to take security corrective actions.
 - 8.1.2.1.1 If appropriate for disciplinary or adverse actions, recommendations and actions should be provided in accordance with the NASA Human Capital policies and requirements.
 - 8.1.2.1.2 If potential for criminal action, information to the OIG for investigative and follow-up actions should be provided in accordance with the OIG policies, requirements and procedures.

8.1.3 *The ISO shall:*

- 8.1.3.1 Ensure that subscriber agreements signed by an individual to obtain a NASA PKI certificate include the personnel sanctions that may apply for violation of that agreement.
- 8.1.3.2 Ensure formal sanctions are imposed for personnel failing to comply with these information security policies and procedures.
- 8.1.3.3 Report information security violations by NASA Government or contractor employees to appropriate organizations and officials, and if appropriate to the SOC as a security incident.

9 Organizationally Defined Values

The following table provides the values defined in *NIST SP 800-53* as being at the discretion of the implementing organization. The Section, and Parameter columns are intended to help navigate various *NIST SP 800-53* security controls for easier application of the organizationally defined values; these columns are defined as follows:

- Section: Values in this column indicate whether an organizationally defined value is in the main body of the control (Main), or part of one of the control's enhancements (E1, E2, etc).
- Parameter: Sometimes, a specific Section may have multiple organizationally defined values. In those instances, the bracketed number Parameters indicate which organizationally defined value (numbered sequentially) is being referenced. In the case of nested organizationally defined values, a series of bracketed numbers is used.

Family	#	Name	Section	Parameter	Type	Description	Low	Moderate	High
PS	01	Personnel Security Policy and Procedures	Main	[1]	Frequency	Policy and procedure review.	1/Year	1/Year	1/Year
PS	02	Position Categorization	Main	[1]	Frequency	Review and revision of position risk designations.	1/10-Years	1/10-Years	1/5-Years
PS	03	Personnel Screening	Main	[1]	Reference	List of conditions requiring rescreening.	1. Upon position assignment change when the change involves moving to a higher risk level position 2. When the position risk level of the incumbent's position is elevated. 3. 1/10-Years	1. Upon position assignment change when the change involves moving to a higher risk level position 2. When the position risk level of the incumbent's position is elevated. 3. 1/10-Years	1. Upon position assignment change when the change involves moving to a higher risk level position 2. When the position risk level of the incumbent's position is elevated. 3. 1/10-Years

ITS Handbook (ITS-HBK-2810.13-01) -
Personnel Security -

Family	#	Name	Section	Parameter	Type	Description	Low	Moderate	High
PS	05	Personnel Transfer	Main	[1]	Reference	Transfer or reassignment actions.	1. Open new accounts and close old accounts. 2. Change system authorizations. 3. Return of, and issue new, keys, building passes, etc. 4. Transfer of individual access to official records needed by the employee at new position/location.	1. Open new accounts and close old accounts. 2. Change system authorizations. 3. Return of, and issue new, keys, building passes, etc. 4. Transfer of individual access to official records needed by the employee at new position/location.	1. Open new accounts and close old accounts. 2. Change system authorizations. 3. Return of, and issue new, keys, building passes, etc. 4. Transfer of individual access to official records needed by the employee at new position/location.
PS	05	Personnel Transfer	Main	[2]	Time Period	Window for performing transfer or reassignment actions.	2 Days (Working)	2 Days (Working)	2 Days (Working)
PS	06	Access Agreements	Main	[1]	Frequency	Review and update of access agreements.	1/Year	1/Year	1/Year